# Citadel Chambers

## MANAGING DATA PROTECTION BREACHES

There are four key steps to the Chambers' data protection breach management plan:

1. Containment and recovery
2. Assessment and ongoing risk
3. Notification of breach
4. Evaluation and response

**1. Containment and recovery:**

**Data Protection Manager(DPM)** and reporting person must:

1. Take steps to recover any lost data and limit the damage that the breach can cause where possible;
2. Decide who will lead the investigation into the breach; and
3. Find out who needs to be aware of the breach and tell those persons what they are expected to do (if anything) to assist in the containment and recovery of the breach.

**2. Assess the risks**

The person leading the investigation must assess the potential adverse consequences of the breach for the individuals concerned (the individuals to whom the personal data in question pertains), the potential severity or scale of the breach and the likelihood of adverse consequences occurring.

**3. Notification of breaches**

The DPM will notify and joint data controller immediately .This policy will in such circumstances be implemented in liaison with such joint controller

Chambers has a duty to report all data protection breaches that are likely to result in a risk to the rights and freedoms of individuals to the Information Commissioner's Office (ICO).

The **DPM, John Binks** or a suitable deputy in his absence, is responsible for ensuring that all relevant data protection breaches are reported to the ICO without delay and no later than 72 hours after having become aware of it.

The **DPM** will report the breach to the ICO in accordance with the reporting methods set by the ICO.

Where deemed appropriate, the individuals affected by the data protection breach must also be informed. The investigating person must provide individuals with specific and clear information about what has happened and what is being done to address the breach. Advice should also be offered on any steps that the affected individuals can take to protect themselves. The individuals must be given contact details should they require further information or help.

Considerations must also be made as to whether any other third parties should be notified, including, for example., the Police, insurers, professional bodies, banks etc.

**4. Evaluation and response**

The final step is to evaluate the Chambers' response to the data protection breach.

It is important to establish whether the breach was caused by an isolated incident or is part of a wider systemic issue so that Chambers can try to prevent the same or a similar breach from occurring in the future.

Any lessons learned should be shared across Chambers as appropriate by communicating the details to the relevant members and staff of Chambers.

The **DPM** will review all /any records of data breaches periodically to establish any trends requiring further attention.

**RECORDING A DATA PROTECTION BREACH**

There must be a central record of all data protection breaches that occur. John Binks DPM is responsible for maintaining a data protection breach register.

John Binks
Citadel